Architecture and Security Technical Standards List			
Original Effective Date:	02/23/04	**Release:**	1.1
Effective Period:	02/23/04 – Current	**Status:**	Approved

The following is a list of high-level architecture and security standards intended as a tool to be used by the State of Wisconsin Department of Health and Family Services' (DHFS) divisions/offices and the Bureau of Information Systems (BIS) when obtaining a vendor's technical proposal and assessing how well it fits the DHFS environment.

When a division/office creates any type of document to solicit IT products or services (such as a Request for Proposal (RFP), Request for Service (RFS), Request for Bid (RFB), or Request for Information (RFI)), BIS will assist in ensuring the technical information is clearly specified and any special handling is identified.

This list should be included in any Request, and the Request should require vendors to respond with a description of how they meet/comply with the requirements listed. Vendors must provide additional information, including version numbers and alternatives, especially where the proposed solution does not fit the applicable standards below.

This list defines the infrastructure within DHFS. This list may be extended if business needs require access from outside of DHFS (such as from the County systems).

When a division/office receives a vendor's response, the division/office should seek the input of BIS in evaluating the response prior to awarding the contract. This will ensure the vendor is in compliance with DHFS' policies and standards, as outlined in this document and on the DHFS WorkWeb (our Intranet site) at:
http://dhfsweb/it/Policies/Policies&Standards/ITPolicy.htm.

In cases where a division/office has a business need requiring a solution that does not meet with the published DHFS standards and/or policies, BIS can work with the division/office to explore options for implementation including assistance in selecting the appropriate vendor and/or products.

Items in {} indicate planned version changes and a probable effective date (by Quarter based on calendar year). It is best to plan for both the current version and the {planned version, date} for each relevant item. Note planned version numbers and dates may change.

Supported Solution Technologies for DHFS:

1) **Web Applications**
   a) Authentication / Identification
      i) Use existing State-wide e-Business Directory (LDAP – Lightweight Directory Access Protocol)
      ii) Unique User Ids and Passwords

   b) Database
      i) Oracle v8.1 {Oracle 9i, Q3 2004}

   c) Development

i) Java, J2EE, OS-independent, browser-independent

d) Hosting
   i) IBM WebSphere 4.0

e) Browser
   i) I.E. 5.5 {I.E. 6, Q1 2005}

f) Messaging
   i) Novell GroupWise v.6 {GroupWise v.6.5, Q3 2004}
   ii) IBM MQ Series

g) Data Transmission
   i) HTTPS, SSL v3, 128bit
   ii) HTTP
   iii) BDE Protocol {Valicert Secure Transport, Q2 2004}

2) Client-Server Applications

a) Authentication / Identification
   i) Unique User Ids and Passwords
   ii) Novell e-Directory

b) Custom-built Applications
   i) Novell e-Directory
   ii) Databases:
      (1) Oracle v8.1 {Oracle 9i, Q3 2004}
      (2) SQL Server 2000
      (3) MS Access 97 for workgroup solutions only (Workgroup is defined as databases and applications confined to a single server, with 5 or fewer concurrent users at the same geographical location.) {MS Access 2003, Q1 2005}

3) Desktop

a) Windows NT 4 {Windows XP, Q1 2005}
b) MDAC v2.1 {MDAC v2.6.2, Q2 2004} {MDAC v2.7, Q1, 2005}
c) Microsoft Office 97 {Office 2003, Q1 2005}
d) Novell GroupWise client v6 {GroupWise client v.6.5, Q3 2004}

4) Server

a) Windows 2003
b) Sun Solaris

5) LAN/WAN

a) TCP/IP
b) SNMP

6) HIPAA Compliance

a) All applications built for programs that must be HIPAA-compliant should reference the requirements published at: http://aspe.os.dhhs.gov/admnsimp/.

7) American Disabilities Act Compliance

a) All applications should reference the requirements regarding accessibility in standards 604 through 607 at the intranet site http://enterprise.state.wi.us/home/standards/.

8) Access Control Definitions

a) Discretionary Access Control

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a user or process given discretionary access to information is capable of passing that information along to another subject.

b) Role-Based Access Control

An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform the role.

9) Deployment Requirements

a) Additional Component Specifications

i) Any additional components required for the working of the proposed system must be listed.

ii) Vendors should include details regarding how their proposed system is compatible with all other components listed in this document.

b) Deployment Processes

i) Vendors should include any information on deployment processes, prerequisites, etc, which may effect the deployment of the proposed system.

c) Vendors should include capacity requirements for the following:

i) Server Disk
ii) Server Memory
iii) Transaction Speed/Network Speed
iv) Client Disk
v) Client Memory
vi) Anticipated Growth

10) Security

a) See sections on Authentication, Identification, HIPAA, and Access Control

11) Mainframe

a) Operating Platform: OS390
b) Database: DB2
c) Security: RACF
d) Authentication and Identification: Unique User Ids and Passwords

12) Hardware

No non-delegated hardware (contact DHFS IT Acquisition Manager for current list) should be purchased or acquired on behalf of DHFS before being reviewed and approved by the DHFS CIO, if the hardware will be connected to the DHFS network.

DHFS hardware standards are suitable for fully supporting the standards listed in this document. Vendors must include hardware requirements in their responses so the solution can be evaluated thoroughly for its fit in the DHFS environment. In some cases, hardware will require a more extensive approval process or an exception before a vendor's solution can be accepted. Hardware outside the DHFS standards noted may be denied. These standards and the contracts available for this procurement change frequently.

See the Desktop, Laptop and Printer Hardware Standards for hardware standards.
http://dhfsweb/it/Policies/Policies&Standards/3_01_Desktop_Hardware/3-1-pb.pdf

Problematic Technologies

Vendors should avoid proposing solutions outside the DHFS standards. Any proposals using the following technologies will need additional justification and review and may be denied. This list is generalized and intended as a guideline only and is not meant to be all-inclusive. Please contact BIS with specific questions.

1) The following implementations are not compatible with current infrastructure, standards, and best practices:

a) Applications requiring a separate account store or directory.
b) Applications requiring separate security systems or that do not uniquely identify users.
c) Solutions built on operating systems or database platforms not noted above.
d) Solutions requiring desktops to have modems.
e) Solutions with network interface cards bridging a foreign network and the DHFS network.

2) The following solutions require additional vendor/business justification and/or investigation to determine compatibility:

a) Resource-intensive solutions that could potentially exceed the capacity of the network beyond a manageable amount (example: streaming video on the network).
b) Solutions requiring remote connection software or desktop client software.
c) Applications with highly specialized support requirements.
d) Solutions requiring .NET services.

Approved by Denise Webb, DHFS CIO on February 23, 2004